Radboud Universiteit Nijmegen

Stealth Sms

Description of how it works

Auteur:
Bart Lutgens

Begeleider:
Prof.dr. B.P.F. Jacobs

27 Juni 2011

Afstudeernummer 652

Table of Contents

Hoofdstuk 1

Inleiding

Een recente ontwikkeling, die de recherche geholpen heeft bij het arresteren van enkele verdachten, is een techniek, die onofficieel een “stealth sms” genoemd wordt. Andere namen zijn “stille sms” of “onzichtbare sms”. De recherche stuurt een dergelijk stealth sms naar de telefoon van een verdachte, waarna de telefoon van de verdachte GPS coördinaten terug stuurt. Dit gebeurt allemaal zonder dat de telefoon aan de verdachte laat weten wat er gebeurd.

Omdat deze techniek nog vrij recent is, is het nuttig om uit te zoeken hoe het hele proces precies in zijn werk gaat. Tijdens dit onderzoek zullen de sterke en zwakke punten zichtbaar worden. Hierop kan de techniek dan mogelijk verbeterd worden. Hoe zit het bijvoorbeeld met de beveiliging van dit systeem? Is er überhaupt wel een beveiliging? Naast deze beschrijving zal er ook een beschrijving zijn met voor- en nadelen tegenover andere traceermethodes zoals de driepuntsmeting.

Als product verwacht ik hierbij een beschrijving van de technieken die gebruikt worden in dit proces en antwoord op mogelijke deelvragen als: Hoe blijft de sms onzichtbaar? Hoe verstuurt de targettelefoon een sms terug? Hoe komt de telefoon aan de huidige GPS locatie?

Om deze beschrijving te maken zal ik antwoord proberen te geven op de volgende onderzoeksvraag:

HOOFDSTUK 1 INLEIDING

“Hoe werkt de techniek achter plaatsbepaling met behulp van een stealth sms en wat zijn de voor- en nadelen tegenover eerder gebruikte telefoon traceer methodes?”

Als deze techniek echt zo goed is, als gezegd wordt, dan wil ik wel eens uitzoeken hoe het dan precies in zijn werk gaat. Omdat ik interesse heb ik communicatie en security, leek me dit een geschikt onderwerp.

Dit hele systeem werkt op basis van de GPS locatie van de telefoon. Met behulp van de satellieten, die rond de aarde draaien kan een GPS ontvanger bepalen ‘waar op aarde’ hij zich bevindt. Deze ontvangers zitten tegenwoordig op heel veel moderne mobiele telefoons. De precieze plaats op de aarde wordt beschreven in een set van coördinaten. De stealth sms’jes sturen deze set coördinaten terug naar de recherche.

Ik ben van plan dit onderzoek op te delen in een aantal stukken, die ik apart ga beschrijven.

Ten eerste (en naar mijn mening het belangrijkste), hoe blijft de sms onzichtbaar. Normaal gesproken als een sms binnenkomt op een telefoon dan krijg je op zijn minst een notificatie te zien van deze sms. In (in deze situatie) slechtere gevallen trilt de telefoon ook en wordt er een geluid afgespeeld. Dit is natuurlijk niet de bedoeling. Ik vraag me daarom af hoe de verstuurder van de stealth sms ervoor zorgt dat er geen melding van de nieuwe sms komt bij de ontvanger.

Ten tweede, hoe krijgt de telefoon de coördinaten die verstuurd moeten worden. Normaal gesproken moet je om je huidige locatie te bepalen een applicatie starten, die dit doet. Deze applicatie is bij veel telefoons standaard, maar niet altijd actief. De vraag is dus, hoe de telefoon in zijn stand-by status de GPS locatie kan bemachtigen zonder dat de telefoon uit de stand-by status *lijkt* te gaan.

Ten derde, hoe verstuurt de telefoon de GPS locatie, nadat hij deze bemachtigd heeft, weer (1 keer? Elk uur?) onzichtbaar terug? Eigenlijk kijk ik hier weer naar

het probleem, dat in de eerste 2 deelvragen ook essentieel is, hoe blijft dit allemaal onopgemerkt door de gebruiker van deze telefoon?

In deze eerste 3 deelvragen zoek ik uit hoe het gehele proces in zijn werk gaat. Hiernaast wil ik ook nog uitzoeken hoe deze techniek werkt ten opzichte van de andere technieken zoals de driepuntslocatie. Wat zijn de verschillen en wat zijn de voor- en nadelen van deze techniek?

Als laatste wil ik nog graag kijken naar enige security aspecten van deze techniek. Bij deze security hoort in elk geval (naar mijn mening) een soort autorisatie, anders kan iedereen met de nodige software stealth sms'jes gaan versturen. Maar de vraag is of deze of andere security methoden wel gebruikt worden?

De deelvragen zijn dan:

"Wat is de techniek achter het versturen van een onzichtbare sms naar een targettelefoon?"

"Hoe verwerkt de telefoon deze sms en bemachtigd een GPS locatie zonder dat de gebruiker dit door heeft?"

"Hoe verstuurt de targettelefoon een sms met de benodigde informatie die onzichtbaar is op de targettelefoon maar leesbaar op de brontelefoon(telefoon van de recherche)?"

"Wat zijn de voor- en nadelen en wat zijn de verschillen tussen deze techniek en andere traceertechnieken?"

"Welke security methoden worden door dit systeem gebruikt en welke methoden zouden er gebruikt moeten worden?"

Hoofdstuk 2

The sms-protocol

Om te achterhalen hoe het versturen en ontvangen van stealth sms'jes in zijn werk gaat, zal ik eerst naar de basis moeten kijken. In dit geval is dat het protocol achter het versturen en ontvangen van sms'jes. Sms, short message service, is een dienst waarbij je met behulp van een mobiele telefoon, of een ander communicatie systeem van eenzelfde aard, een kort tekst bericht kunt versturen of ontvangen over het sms-protocol.

Dit zogenaamde communicatie protocol is een formele beschrijving van de verschillende regels en formats, waaraan een tekst bericht en de connectie tussen (in dit geval) 2 mobiele telefoons moeten voldoen, zodat het tekst bericht in de juiste staat bij de juiste ontvanger terecht komt.

Sms berichten die verstuurd worden, worden verwerkt in de zogenaamde short message service centers. Deze SMSC's worden door de verschillende service providers (KPN, T-Mobile, etc.) onderhouden.

Wanneer een SMSC een bericht wil versturen naar de ontvanger kunnen twee technieken gebruikt worden. De store-and-forward of de store-and-forget. In het eerste geval probeert de SMSC het bericht te versturen naar de ontvanger en als de ontvanger niet bereikbaar is, dan wordt de sms in een wachtrij gezet, zodat op een later tijdstip een nieuwe poging om te verzenden gedaan kan worden. In het tweede geval gaat de sms verloren, wanneer de ontvanger onbereikbaar is.

Een dergelijk SMSC kan een sms bericht versturen met een maximale grote van 140 octets (bytes). Zo kan een sms bericht waarin 1 teken gecodeerd wordt met behulp van een 8-bit codering uit 140 tekens bestaan, 160 tekens wanneer gebruikt wordt gemaakt van een 7-bit codering en uit 70 tekens wanneer je een 16-bit codering nodig hebt om 1 teken op te slaan. Deze laatste codering is de UTF-16 codering die nodig voor talen als Japans, Chinees of Koreaans. [3]

Hoewel je van een ontvangen sms alleen maar de inhoud en het telefoonnummer van de verzender te zien krijgt bestaat een sms eigenlijk uit:

- Een header. Hierin staat de informatie voor de SMSC
    - Lengte van SMSC informatie
    - Adrestype
    - Nummer van SMSC
- Informatie van de verzender
    - Adrestype
    - Nummerlengte
    - Nummer van verzender
- Een protocol identifiër
- De gebruikte codering
- Een tijdcode van het versturen vanuit het SMSC
- De lengte van het verzonden bericht
- De inhoud van het bericht (Dus maximaal 140 bytes)[2]

Aan één of meerdere van deze waardes kan echter wel gesleuteld worden, wanneer je de juiste technieken hebt.

De enige waardes die je normaal gesproken kan zien, wanneer je een sms bericht in de normale textmode ontvangt, zijn de inhoud van het bericht en het nummer van de verzender.

Een tweede manier om sms berichten te versturen en te ontvangen is de PDU (Protocol Description Unit) modus. In de PDU modus werk je met behulp van een bit stream die het sms bericht moet voorstellen. Deze bit stream is dan niet meer

als het aan elkaar plakken van de verschillende configuraties en informatie die je wilt versturen. Sinds je beschikking hebt over de volledige bit stream bij het versturen en ontvangen van berichten is dit een goede modus om in het volgende hoofdstuk verder naar te kijken.

Om duidelijk te maken hoe deze PDU modus in elkaar zit, zal ik nu een voorbeeld geven van een bit stream van een ontvangen bericht:

07911326040000F0040B911316546271F60000115031223572400AE8329BFD4697D9EC37

Om te begrijpen wat hier staat, moet je eerst weten in welk format je deze stream moet lezen. In dit geval staan 2 getallen (of letters) samen voor 1 8-bit octet. Het eerste getal (of letter) staat voor de linkse 4 bits en het tweede getal (of letter) staat voor de rechtse 4 bits. Sinds je met 4 bits een maximale decimale waarde van 15 kan maken, is elk van de 2 getallen een los hexadecimaal getal.

Het bericht bestaat uit 2 delen. Namelijk het deel met de informatie voor het SMSC en het deel met de informatie voor de ontvanger. Om te vinden waar deze splitsing zich plaats vindt, kijk je eerst naar het eerste hexadecimale 8-bit octet. In dit geval 07. Wanneer je dit omschrijft naar een binair getal krijg je:

07 ⟶ 0 7 ⟶ 0000 1000 ⟶ 00001000

00001000 staat natuurlijk weer gelijk aan 7 decimaal. Je weet dan dat er na het eerste octet nog 7 octets gebruikt worden om informatie op te slaan over de SMSC. De eerste ontleding ziet er dan als volgt uit:

07
911326040000F0
040B911316546271F60000115031223572400AE8329BFD4697D9EC37

Wanneer je op een zelfde manier door gaat met ontleden blijft uit eindelijk deze betekenis over:

07	Lengte van de SMSC informatie. In dit geval 7 bytes
91	Adres type van de SMSC. In dit geval betekend 91 internationaal
13 26 04 00 00 F0	Het nummer van het SMSC. Het telefoonnummer is oneven dus laatste F is toegevoegd om passende bytes te maken. In dit geval is het nummer +31624000000 (T-Mobile)
04	Hier begint de sms data
0B	De lengte van het telefoonnummer van de zender. In dit geval 11 (landcode zorgt voor het extra nummer) (B hexadecimaal is 11 decimaal)
91	Adrestype van het zendernummer
13 16 54 62 71 F6	Het nummer van de zender. In dit geval +31614526176 (mijn nummer)
00	Protocol Identifiër. In dit geval is 00 is het standaard SME-to-SME protocol waarbij SME (short message entity) een verzamelnaam is voor alle externe apparaten die sms berichten kunnen ontvangen, zoals een mobiele telefoon
00	Gebruikte codering, volgens het Data Coding Scheme
11 50 31 22 35 72 40	De tijdcode van het versturen vanuit het SMSC. YY MM DD HH MM SS TIJDZONE (in stappen van 15 minuten) In dit geval is dat dus: 2011 Mei 13, 22:53:27 GMT +1
0A	Lengte van het bericht. In dit geval 10 tekens (septets, want codering is 7-bit)
E8329BFD4697D9EC37	Het bericht “hellohello”

Zoals je kunt zien komt de ontleding overeen met de onderdelen die een sms bericht bevat.

Hoofdstuk 3

The workings of stealth

Om erachter te komen hoe een bericht verstuurd kan worden zonder dat de ontvanger hier achter komt kunnen we op verschillende plaatsen in het sms-protocol kijken. Na verder onderzoek is echter gebleken dat de eerdere nieuwsberichten over dit nieuwe fenomeen sterk overdreven zijn. Wanneer we praten over een stealth sms, dan gaat het eigenlijk over een ping naar een telefoon. Hoewel deze ping inderdaad niet te detecteren is op de ontvangende telefoon, bevat deze ping ook geen verdere commando's of informatie die verwerkt kan worden.

Er zijn verschillende manieren om een dergelijke ping naar een telefoon te sturen:

3.1 Empty Flash SMS

Een eerste plek om te kijken, zijn de verschillende klassen waaruit een sms kan bestaan. De klasse van een sms bericht bepaald de prioriteit van het bericht en

de locatie waar het bericht opgeslagen moet worden. De verschillende klassen zijn:

- Class 0: Sms berichten met deze klasse moeten direct op de mobiele telefoon direct getoond worden. Er wordt direct een status rapport terug gestuurd naar het SMSC. Een bericht met deze klasse wordt niet automatisch op de mobiele telefoon of SIM kaart opgeslagen, dit gebeurt alleen met specifieke instructie van de ontvanger
- Class 1: Berichten met klasse 1 zijn de “normale” sms berichten. Deze berichten komen binnen in de inbox en worden opgeslagen op de mobiele telefoon of SIM kaart volgens de configuratie van de mobiele telefoon
- Class 2: Sms berichten met klasse 2 zijn berichten die data bevatten die opgeslagen moet worden op de SIM kaart. Een status rapport van dit soort berichten wordt pas verzonden nadat de data gekopieerd is naar de SIM kaart (wanneer mogelijk)
- Class 3: Dit zijn berichten die direct doorgestuurd worden van de mobiele telefoon naar een extern apparaat. Een status rapport wordt in ieder geval teruggestuurd naar het SMSC, zodra het bericht op de mobiele telefoon binnenkomt, hoewel er niet gecontroleerd wordt of het doorsturen succesvol was.[5]

Een class 0 sms, ook wel een flash sms genaamd, lijkt een goede start. Deze berichten komen direct op het scherm te staan en worden niet opgeslagen. Wanneer je een flash sms stuurt zonder inhoud, heb je al een manier te pakken om een stealth sms te versturen. Hoewel er tegenwoordig nog maar weinig telefoons zijn waarbij je vanuit de telefoon kan instellen om je sms als flash sms te versturen, zijn er genoeg gratis ‘3th party freeware clients’ beschikbaar om je flash sms over het internet te versturen. Ook zijn er ‘3th party software updates’ voor onder andere windows mobile waarbij de optie om flash sms te versturen beschikbaar is.

Deze '3th party clients' of software updates van mobiele telefoons maken handig gebruik van de PDU modus om sms berichten te versturen. De PDU modus geeft namelijk ook status updates weer bij het versturen om een sms bericht. Één van de notificaties, die volgt na het versturen van een bericht, is de bevestiging van ontvangst.

3.2 Manipulation of the data coding scheme

Bij de tweede manier voor het versturen van een stealth sms moeten we gebruik maken van de mogelijkheid om configuraties aan te passen bij het versturen van een sms bericht.

Zoals eerder besproken is één van de opties, die een verzender moet kiezen bij het versturen van een sms bericht, de manier waarop de inhoud gecodeerd wordt. Deze configuratie wordt het data coding scheme genoemd.

De configuratie van het data coding scheme wordt bepaald door 8 bits die, wanneer verzonden via de PDU modus, worden weergegeven als een hexadecimaal octet.

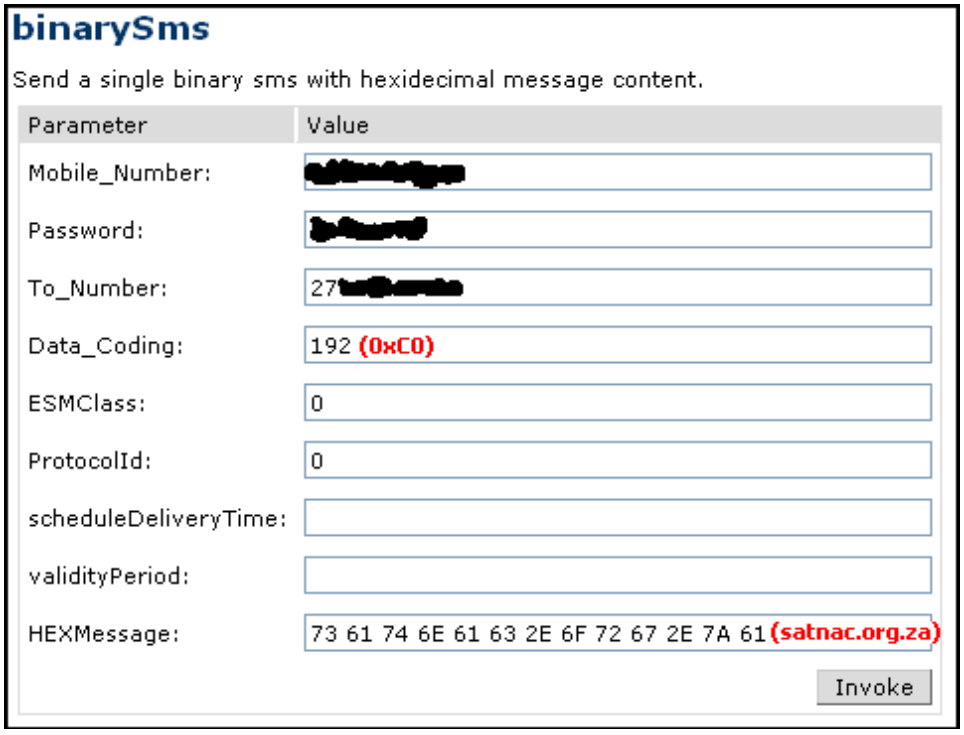
Van deze 8 bits bepalen de linkse 4 bits wat voor soort bericht verstuurd moet worden. In elk van de verschillende soorten berichten hebben de rechter 4 bits andere betekenissen. De verschillende soorten berichten die verstuurd kunnen worden zijn alsvolgt:[6]

00xx	Een normaal bericht. Met behulp van de overige 6 bits kan onder andere bepaald worden welke codering van de inhoud gebruikt moet worden (7 bit, 8 bit of 16 bit) door bit 3 en 2 en welke klasse het bericht heeft door bit 1 en 0.
1100	Discard message. De overige 4 bits hebben dezelfde functie als bij een normaal bericht, hoewel hier door de ontvangende telefoon niet naar gekeken wordt. Het bericht wordt namelijk

	door de ontvangende telefoon zonder op te slaan weggegooid.
1101	Een indicatie bericht. Hiermee kan een telecom provider de ontvangende telefoon notificeren dat er een bericht in de wacht staat. Met behulp van de overige bits wordt het type bericht dat in de wacht staat aangeduid. Het gaat hier dan bijvoorbeeld om een fax bericht of een voicemail bericht.

Wanneer je dus een flash sms met klasse 0 wilt versturen is dit ook mogelijk door het data coding scheme te manipuleren.

Waar het in deze tweede manier van het versturen van een stealth sms om gaat is natuurlijk de tweede groep. Voor het gemak kiezen we voor de rechts bits even 0000. Je krijgt dan 1100000. Wanneer we dit omschrijven naar een hexadecimaal 8-bit octet krijgen we C0. (192 decimaal)



(3th party client)

Wanneer dit bericht zo verstuurt, krijg je de volgende status updates van de PDU modus:

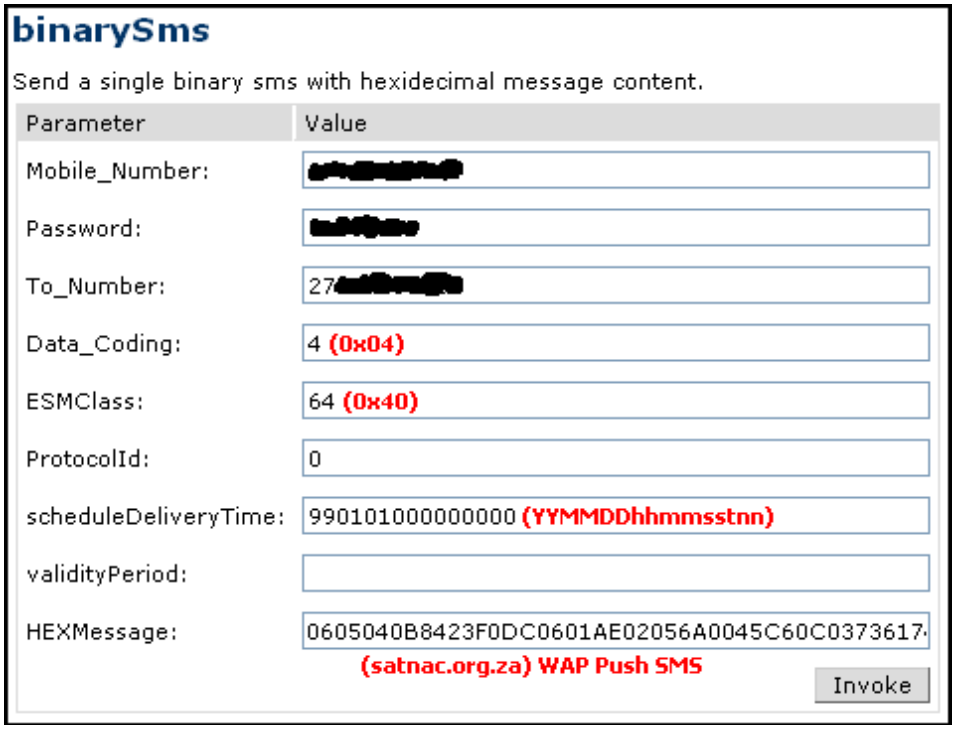
```
2007-04-14 11:45:38  ### INFORMATION: [27829239812] => [27829239812] => [PAIDFOR]
2007-04-14 11:45:38  ### INFORMATION: PDU hex:
00-00-00-44-00-00-00-04-00-00-00-00-00-00-02-C3-00-05-00-32-37-38-32-39-32-33-39-
38-31-32-00-01-01-32-37-38-32-39-32-33-39-38-31-32-00-00-00-00-00-00-01-00-C0-00-
13-73-61-74-6E-61-63-2E-6F-72-67-2E-7A-61
2007-04-14 11:45:38  ### INFORMATION: SubmitSmResp received: -111187017-
2007-04-14 11:45:57  ### INFORMATION: DR received: id:111187017 sub:001 dlvrd:001
submit date:0704141145 done date:0704141145 stat:DELIVRD err:000 text:
```

Het bericht staat inderdaad als afgeleverd, maar er is op de ontvangende telefoon geen bericht te zien.[2]

3.3 Manipulating the timing

De derde en laatste manier om een stealth sms te versturen, werkt door de tijdcode van een te versturen sms ongeldig te maken. Dit kan je gemakkelijk doen door een tijdcode te kiezen van een eerdere datum.

Zoals in het vorige hoofdstuk gezien wordt de tijdcode van het versturen van een bericht weergegeven als YY MM DD HH MM SS TIJDZONE (in stappen van 15 minuten). Wanneer je dan voor het eerste hexadecimale octet, dat dus het jaar bepaald, kiest voor een eerder jaar en vervolgens de rest naar wenst invult zal er een stealth sms verstuurd worden.



In dit geval is er gekozen voor de datum 1 januari 1999 om 00:00:00 Gmt 0.

Wanneer je dan kijkt naar de status updates die worden weergegeven in de PDU modus, dan zie je dat het bericht afgeleverd is, hoewel er op de ontvangende telefoon geen bericht te zien was. [2]

```
2007-04-14 12:22:26  ### INFORMATION: [27829239812] => [27829239812] => [PAIDFOR]
2007-04-14 12:22:26  ### INFORMATION: PDU hex:
00-00-00-6E-00-00-00-04-00-00-00-00-00-00-02-D2-00-05-00-32-37-38-32-39-32-33-39-
38-31-32-00-01-01-32-37-38-32-39-32-33-39-38-31-32-00-40-00-00-39-39-30-31-30-31-
30-30-30-30-30-30-30-30-30-00-00-01-00-04-00-28-06-05-04-0B-84-23-F0-DC-06-01-AE-
02-05-6A-00-45-C6-0C-03-73-61-74-6E-61-63-2E-6F-72-67-2E-7A-61-00-01-03-68-69-00-
01-01
2007-04-14 12:22:26  ### INFORMATION: SubmitSmResp received: -111194450-
2007-04-14 12:22:57  ### INFORMATION: DR received: id:111194450 sub:001 dlvrd:001
submit date:0704141222 done date:0704141222 stat:DELIVRD err:000 text:
```

Hoofdstuk 4

Tracking the location

Hedendaags zijn er verschillende manieren om de locatie van een mobiele telefoon te bepalen. De belangrijkste twee zijn: het traceren van een mobiele telefoon via GPS en het traceren via GSM masten.

4.1 GPS Tracking

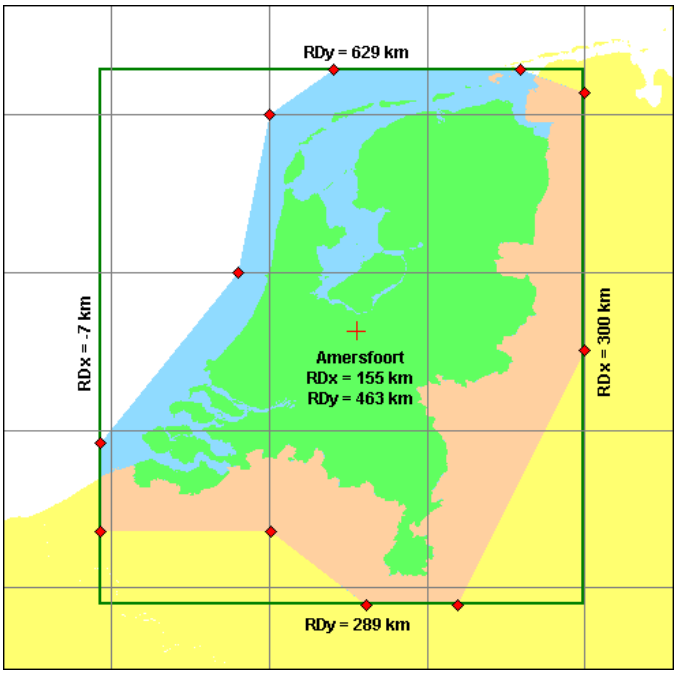
Het GPS, Global Positioning System, is een systeem voor onder andere plaatsbepaling op aarde. Het GPS systeem gebruikt 32, bij de opstart 24, satellieten in 6 verschillende banen om de aarde, die elk een eigen signaal uitzenden. Om de plaats op aarde te berekenen, moet de GPS ontvanger minimaal in contact zijn met 4 van deze satellieten.

De precieze locatie, op 10 meter nauwkeurig, wordt berekend door een afstandsmeting tussen de ontvanger, ergens op de aardoppervlakte, en de verschillende satellieten. Omdat elke satelliet een eigen signaal uitzendt en deze satellieten elk een eigen vaste baan om de aarde hebben met een eigen vaste snelheid, is van elke satelliet altijd bekend waar in de ruimte deze zich bevindt. Wanneer je zo de verschillende, minimaal 4, afstanden tussen de ontvanger en de satellieten analyseert, kun je de positie van de ontvanger bepalen. De positie

van deze GPS ontvanger wordt dan weer gegeven in lengte en breedte coördinaten of kan binnen Nederland ook worden weergegeven in de zogenaamde Rijksdriehoekscoördinaten.

Lengte en breedte coördinaten zijn globaal. De plaats op aarde wordt bepaald op een raster, waarbij het aardoppervlakte als 2-dimensionaal vlak gezien wordt, een cartesisch coördinatenstelsel. De verticale nul-lijn is de meridiaan van Greenwich, waarbij elke plaats ten oosten van deze meridiaan gezien wordt als oosterlengte en elke westerse plaats als westerlengte. De evenaar is de horizontale nul-lijn met elke plaats ten noorden als noorderbreedte en elke plaats ten zuiden als zuiderbreedte.

Het Rijksdriehoeksstelsel is een nationale plaatsbepaling gebruikt in Nederland. Ook dit stelsel volgt de regels van een cartesisch coördinatenstelsel, waarbij de oorsprong, het nul-nul punt, de Onze Lieve Vrouwentoren in Amersfoort was. Om er echter voor te zorgen dat elk punt in Nederland een positieve waarde heeft, is er een translatie toegepast van 155 km naar het westen en 463 km naar het zuiden. Deze translatie zorgt er ook voor dat de minimale y-waarde groter is dan de maximale x-waarde. De x-waardes van Nederland liggen dan tussen 0 en 300 km en de y-waardes tussen 300 en 620 km.



Het domein van alle geldige waardes, RD-coördinaten, ligt tussen de -7 en +300 voor de x-waardes en 289 en 629 voor de y-waardes.

4.2 GSM tracking

Het traceren van een mobiele telefoon met behulp van GSM masten gebruikt geen afstandsmeting maar meting van de sterkte van het GSM signaal. In tegenstelling tot GPS locatie bepaling, waarbij je minimaal 4 metingen nodig hebt om een locatie te kunnen bepalen heb je in dit systeem maar 3 metingen nodig. Door de hoek waarop het GSM signaal de toren binnen komt, Angle of Arrival, wordt bepaald in welk gebied ten opzichte van de eerste GSM mast de mobiele telefoon zich ongeveer bevindt.

Wanneer het GSM signaal zo door drie verschillende GSM masten, die het dichtst bij de mobiele telefoon staan, wordt opgevangen, kan met behulp van de signaalsterkte de positie bepaald worden binnen deze driehoek van masten waar de mobiele telefoon zich bevindt.

De signaalsterkte wordt bepaald door het verschil van ontvangsttijd te meten tussen de GSM masten. De mobiele telefoon stuurt een signaal uit dat door de drie masten wordt opgevangen. Vervolgens wordt de ontvangsttijd van dit signaal door de drie masten vergeleken. Met behulp van de verschillen in ontvangsttijden kan zo een locatie bepaald worden. Deze locatie is nauwkeurig tot 50 meter in dichtbevolkte gebieden (met dus ook een grotere dichtheid van GSM masten).

4.3 Tracking with stealth sms

Hoewel de initiële artikelen en nieuwsberichten leken blijken dat een stealth sms ervoor kan zorgen dat de te traceren telefoon GPS coördinaten terug stuurt, leek dit na verder onderzoek sterk overdreven te zijn.

Hoewel tegenwoordig in veel smartphones een GPS ontvanger aanwezig is, die op verzoek van de gebruiker ook een plaatsbepaling kan geven, is het niet mogelijk deze GPS ontvanger met behulp van een stealth sms te benaderen. In eerste instantie leek het erop, dat een stealth sms, benodigde commando's zou bevatten, die ervoor moeten zorgen dat de GPS ontvanger geactiveerd wordt en, mogelijk met behulp van een sms, GPS coördinaten terugstuurt naar de verzender van de stealth sms. Hoewel er dus geen gebruik wordt gemaakt van het GPS systeem bij het traceren van een target mobiele telefoon, helpt stealth sms wel op 2 manieren.

4.3.1 Cell-Id

Zoals eerder uitgelegd, wanneer je met behulp van de PDU modus een sms bericht verstuurd, dan heb je bij het versturen van een bericht toegang tot statusupdates. Hierin wordt onder andere vermeld wanneer een bericht verstuurd wordt, de totale hex code van het bericht en bevestigingen van ontvangst van de SMSC en de target telefoon. De bevestiging van ontvangst van de targettelefoon bevat onder andere het Cell-Id. Dit is een unieke code waarmee een GSM mast geïdentificeerd wordt. Sinds een mobiele telefoon altijd contact maakt met de GSM mast die het makkelijkst te bereiken is, mag je dus vanuit gaan dat de targettelefoon zich bevindt in het gebied binnen het bereik van de zendmast met het Cell-Id dat je terug krijgt in de ontvangstbevestiging.

Wanneer je veel stealth sms'jes verstuurd in een korte tijd en, afwisselend, verschillende Cell-Ids terug krijgt, helpt dit natuurlijk bij de nauwkeurigheid van de plaatsbepaling. Wanneer de Cell-Ids niet afwisselend veranderen maar geleidelijk van 1 Cell-Id naar een tweede Cell-Id overgaan, kan je ervan uitgaan dat de target mobiele telefoon in beweging is.

4.3.2 Forcing the signal

Wanneer je echter, na een strenge toepassingsprocedure, waarbij onder andere naar het delicttype van de verdachte wordt gekeken, toestemming hebt van het openbaar ministerie om geavanceerde technieken toe te passen, dan is het vaak nuttig om te beginnen met een stealth sms. Met toestemming van het openbaar ministerie krijg je namelijk medewerking van de serviceaanbieder. Met deze medewerking is het mogelijk om een driepuntsmeting toe te passen. Zoals eerder uitgelegd maakt een driepuntsmeting gebruik van verschillende GSM masten om de locatie te bepalen. Je moet echter wel weten bij welke GSM masten je moet zoeken naar de target mobiele telefoon. Na het sturen van een stealth sms heb je een globaal begin, namelijk het Cell-Id van één GSM mast waar het toestel zich in de buurt bevind.

Wanneer er weinig gebruik wordt gemaakt van de telefoon, kun je een signaal vanaf de target mobiele telefoon forceren door het versturen van stealth sms'jes. Elke ontvangstbevestiging wordt dan namelijk opgepikt door de GSM mast.

Hoofdstuk 5

Evaluation

Om erachter te komen of het traceren van mobiele telefoons met behulp van stealth sms'jes nu inderdaad zo'n goede methode is, zal ik in dit hoofdstuk enkele andere punten evalueren.

Ten eerste zal ik kijken naar de veiligheid van deze techniek. Kan iedereen deze techniek toepassen of wordt de methode beschermd door de overheid?

Ten tweede zal ik kijken naar de verschillen en overeenkomsten, voor- en nadelen tussen deze techniek en enkele andere traceermethoden.

5.1 Security aspects

De techniek waarbij je stealth sms'jes stuurt naar een target mobiele telefoon om vervolgens via het cell-id van de GSM mast met de sterkste verbinding naar deze target mobiele telefoon een globale plaatsbepaling te maken kan door iedereen uitgevoerd worden. Het resultaat is, dat jij als plaatsaanduiding een identificatienummer van een GSM mast krijgt. Hier heb je echter weinig aan, je hebt namelijk geen toegang tot een database met deze cell-ids en hun echte locatie, waar we ervan uit mogen gaan dat de politie en de recherche wel

toegang hebben tot deze informatie. Om dus enig resultaat te krijgen, als 'normaal' persoon, zul je dus een cell-id naar locatie database moeten maken. Wanneer je op het internet gaat zoeken blijkt als snel dat er mensen zijn die dit inderdaad proberen. Wanneer genoeg mensen geholpen hebben, heb je echter alsnog maar een onvolledige, vrij onnauwkeurige database, gebaseerd op onbetrouwbare bronnen.

Wanneer je dus stealth sms'jes wilt versturen om een plaatsbepaling te krijgen van een target telefoon, zul je weinig succes hebben. Het enige dat je kunt bereiken is controleren of de target mobiele telefoon in ongeveer dezelfde omgeving als jezelf is. Je doet dit door een (stealth) sms bericht te sturen naar je eigen telefoon en bij de ontvangstbevestiging naar het cell-id te kijken. Wanneer je nu na het versturen van een stealth sms naar de target telefoon hetzelfde cell-id terug krijgt, weet je dat de target telefoon gebruik maakt van dezelfde GSM mast.

Wanneer je naar de andere technieken van plaatsbepaling kijkt, zoals de driepuntsmeting of het GPS systeem, dan zie je dat deze alleen mogelijk zijn met de juiste apparatuur en/of medewerking van de serviceaanbieder. En deze apparatuur of medewerking wordt alleen aangeboden aan de recherche na toestemming van het openbaar ministerie. Deze technieken vallen dus onder de privacywet en zijn illegaal om als 'normaal' persoon te gebruiken.

5.2 Comparison

Om een vergelijking te maken tussen de verschillende technieken, GPS systeem, driepuntsmeting en stealth sms, moeten er eerst een aantal eigenschappen geïdentificeerd worden waarop de vergelijking zal plaats vinden. Deze eigenschappen zijn: nauwkeurigheid, snelheid en toepasbaarheid.

5.2.1 Accuracy

Zoals eerder uitgelegd is het GPS systeem het nauwkeurigst. De metingen met behulp van de satellieten resulteren in een set coördinaten, die tot op 10 meter nauwkeurig zijn. Hoewel dit niet de precieze locatie geeft, lijkt dit nauwkeurig genoeg om een persoon te kunnen traceren naar een specifiek huis, wanneer de verdachte zich binnenshuis verstopt, of naar een specifieke straat, als de verdachte in beweging is.

Het traceren met behulp van de driepuntsmethode (met mogelijke ondersteuning van stealth sms), heeft een nauwkeurigheid to 50 meter. Hoewel deze nauwkeurigheid waarschijnlijk goed genoeg is om de juiste straat te bepalen waar de verdachte zich bevindt, zal deze techniek niet het juiste huis kunnen vinden. Wanneer je echter, als recherche, een verdachte kan lokaliseren tot op een gebied van 100 meter (cirkel met middelpunt de plaatsbepaling en straal 50 meter) in doorsnede, dan kan er binnen dit gebied gezocht worden naar huizen waar de verdachte een verbinding mee heeft. Omdat dit gebied niet erg groot is, zal de recherche ook met deze techniek succes hebben.

De nauwkeurigheid van de techniek die gebruik maakt van stealth sms is niet duidelijk. Als resultaat van deze techniek krijg je een cell-id. Ervan uitgaande dat je toegang hebt tot de database waaruit je een locatie van de GSM mast kunt halen, dan heb je als plaatsbepaling voor de verdachte een gebied rondom de GSM mast. De grootte van dit gebied ligt echter aan de omliggende GSM masten. Sinds het signaal van de mobiele telefoon via de GSM mast gaat waarbij de sterkste verbinding tot stand gebracht kan worden, loopt het gebied in alle richtingen tot ongeveer halverwege de afstand naar de eerstvolgende GSM mast. Omdat het hier om signaalsterkte gaat en niet om kortste afstand naar de GSM mast, is het ook nog maar de vraag of het signaal naar een toren die dichterbij staat niet slechter is door mogelijke interferentie.

Je hebt dus te maken met een gebied van onbekende grootte dat zich om een GSM mast bevindt. Voor precisielokalisatie is deze techniek dus geen goede

optie. Wanneer je echter naar een globale positie op zoek bent, zoals een bepaalde stad in een land, dan kun je deze techniek wel gebruiken.

5.2.2 Speed

Hoewel de snelheid tot men resultaten heeft in verschillende situaties minder belangrijk is, zoals een verdachte, die zich binnenshuis verstopt, kan het verschil uit maken, wanneer een bewegende verdachte in realtime gevolgd moet worden.

De snelheid van stealth sms is het grootst. Je stuurt een sms en je hebt resultaat met de bevestiging die direct terug gestuurd wordt. Je hebt, zoals eerder uitgelegd, alleen niet veel aan deze techniek bij een bewegende verdachte in realtime.

Het bepalen van een locatie met behulp van driepuntsmetingen en het GPS systeem is wat langzamer. Het benaderen van de verschillende GSM masten of satellieten heeft in eerste instantie wat tijd nodig. Maar zoals je bijvoorbeeld in je navigatiesysteem in de auto merkt, wanneer de eerste berekening bezig is, wordt al een tweede berekening gestart. Dus wanneer je de eerste plaatsbepaling gemaakt hebt, kunnen er realtime updates gedaan worden, zodat een verdachte gevolgd kan worden als hij in beweging is.

De snelheid van deze technieken, samen met de huidige vooruitgangen in hardware, heeft dus weinig tot geen negatief effect.

5.2.3 Applicability

Als we naar de toepasbaarheid van deze technieken kijken vanuit het oogpunt van de recherche, dan blijkt dat driepuntsmetingen en het GPS systeem (mits de recherche hier de apparatuur voor heeft) onder de privacywet vallen. Om de

privacywet te mogen schenden, zal de recherche toestemming moeten hebben van het openbaar ministerie. Deze toestemming wordt niet zomaar gegeven. De toepasbaarheid van de driepuntsmeting en het GPS systeem heeft dus grenzen. Het pingen van de target mobiele telefoon met stealth sms berichten is niet illegaal zonder toestemming van het OM.

5.2.4 Conclusion

Hoewel het pingen met behulp van stealth sms berichten altijd mogelijk is en ook het snelste is, kan de recherche met alleen deze techniek de verdachte niet tot een precieze locatie traceren.

Het bepalen van een locatie van een verdachte met behulp van driepuntsmetingen of het GPS systeem vereist toestemming van het OM, de juiste apparatuur en medewerking van de serviceaanbieder, (die met toestemming van het OM gegeven moet worden) maar is wel nauwkeuriger en zal waarschijnlijk ook leiden naar het vinden van de verdachte. Hoewel deze beide technieken meer tijd kosten, zal dit niet nadelig zijn bij het vinden van de verdachte.

Hoofdstuk 6

Conclusion

De vraag, die ik in dit onderzoek trachtte te beantwoorden was:

“Hoe werkt de techniek achter plaatsbepaling met behulp van een stealth sms en wat zijn de voor- en nadelen tegenover eerder gebruikte telefoon traceer methodes?”

Dit probleem heb ik toen opgedeeld in 5 deelvragen, die ik nu elk apart even kort probeer te beantwoorden met de kennis uit de vorige hoofdstukken.

“Wat is de techniek achter het versturen van een onzichtbare sms naar een targettelefoon?”

Het versturen van de zogenaamde stealth sms is mogelijk op verschillende manieren.

- Het versturen van een zogenaamde lege Class 0 sms, ook wel genaamd flash sms. Deze sms verschijnt (wanneer inhoud aanwezig is) direct op het scherm en wordt niet opgeslagen op de telefoon of SIM kaart.

- Het manipuleren van het data coding scheme. Wanneer de juiste configuratie gekozen wordt, dan discard de ontvangende telefoon het bericht direct zonder naar inhoud of afzender te kijken.
- Het manipuleren van de verzendtijd. Als de tijdcode ongeldig is, door bijvoorbeeld een vroegere tijd in te vullen, dan wordt er geen bericht gestuurd, maar de target telefoon ontvangt wel een ping van het SMSC.

"Hoe verwerkt de telefoon deze sms en bemachtigd een GPS locatie zonder dat de gebruiker dit door heeft?"

Deze vraag samen met de volgende deelvraag was gemaakt naar aanleiding van een overdreven nieuwsbericht en is komen te vervallen.

"Hoe verstuurt de targettelefoon een sms met de benodigde informatie die onzichtbaar is op de targettelefoon maar leesbaar op de brontelefoon(telefoon van de recherche)?"

Hoewel dit, zoals bij de vorige vraag te lezen, niet gebeurd, zal ik hier even kort beschrijven hoe een locatie bepaald wordt met behulp van deze techniek.

Door het versturen van een stealth sms naar een verdachte, wordt de target mobiele telefoon geforceerd een ontvangstbevestiging terug te sturen. Deze bevestiging gaat via een GSM mast. In de informatie die de recherche terug krijgt in de bevestiging is onder andere een cell-id te vinden. Dit is een identificatienummer van een specifieke GSM mast. De recherche heeft dan dus een globale locatie van de target telefoon rondom deze GSM mast.

"Welke securitymethoden worden door dit systeem gebruikt en welke methoden zouden er gebruikt moeten worden?"
Het grootste security aspect van de verschillende technieken is de privacywet. Het pingen van een target telefoon met behulp van stealth sms'jes valt hier echter niet onder. Elke persoon zou dit dus in principe legaal mogen doen. De veiligheid zit hem echter in de geheimhouding van de database waarin cell-id van GSM masten gekoppeld worden aan specifieke locaties.

HOOFDSTUK 6 CONCLUSION

Omdat dit een techniek is die vanuit verschillende types toestellen en zelfs computers toegepast kan worden is daar geen extra security toe te passen. De enige mogelijke verbetering is dat ook het pingen van een mobiele telefoon met stealth sms ook onder de privacywet te laten vallen.

"Wat zijn de voor- en nadelen en wat zijn de verschillen tussen deze techniek en andere traceertechnieken?"

Het traceren van een target mobiele telefoon met behulp van een stealth sms heeft geen toestemming nodig van het Openbaar Ministerie en is dus altijd inzetbaar. De techniek is snel, maar vrij onnauwkeurig.

Het traceren van een target mobiele telefoon met behulp van een driepuntsmeting heeft wel toestemming nodig van het OM om medewerking te krijgen van de serviceaanbieder. Het duurt langer om te meten, maar is wel een stuk nauwkeuriger.

Het traceren van een target mobiele telefoon met behulp van een het GPS systeem heeft ook toestemming nodig van het OM om medewerking te krijgen van de serviceaanbieder. Er is nog extra apparatuur voor nodig en het meten duurt langer. De plaatsbepaling is nog iets nauwkeuriger dan een driepuntsmeting.

Om dan terug te komen op de vraag waar dit onderzoek om draaide:

"Hoe werkt de techniek achter plaatsbepaling met behulp van een stealth sms en wat zijn de voor- en nadelen tegenover eerder gebruikte telefoon traceer methodes?"

Er zijn meerdere manieren om een stealth sms te versturen naar een targettelefoon. Wanneer de recherche zo'n stealth sms stuurt, krijgt de targettelefoon geen melding op het scherm, maar krijgt wel een ping van het SMSC. Op deze ping geeft de targettelefoon een ontvangstbevestiging die via de

HOOFDSTUK 6 CONCLUSION

GSM mast waarbij deze targettelefoon de beste signaalsterkte krijgt wordt verstuurd. Wanneer de recherche deze ontvangstbevestiging terug krijgt staat hier het cell-id in van deze GSM mast. Wanneer dit cell-id gekoppeld wordt aan de specifieke locatie van deze GSM mast, heeft de recherche een globale positie van de verdachte.

De techniek is door iedereen legaal toe te passen, maar alleen met de informatie die de recherche tot hun beschikking heeft kan dit resultaat tot een locatie worden omgezet.

Andere technieken, waarbij de stealth sms soms in ondersteuning wordt gebruikt zijn nauwkeuriger, maar zijn langzamer en hebben toestemming van het Openbaar Ministerie nodig en medewerking van de serviceaanbieder.

Literature

[1] Nieuwsbericht, aanleiding onderzoek. Web reference: https://secure.security.nl/artikel/36059/1/Recherche_vindt_verdachten_via_onzichtbare_sms.html - Februari 2011

[2] N.J Croft and M.S Olivier, *A silent SMS Denial of Service (DoS) attack*. Web reference: http://mo.co.za/open/silentdos.pdf - Februari 2011

[3] Jeff Brown, Bill Shipman and Ron Vetter, *SMS: The Short Message Service* http://www.uncw.edu/itsd/documents/Computer-SMS_pdf.pdf - Maart 2011

[4] Binary Sms, http://mobiforge.com/developing/story/binary-sms-sending-rich-content-devices-using-sms - Maart 2011

[5] GSM Technology http://www.gsm-technology.com/gsm.php/en,unlock,subpage_id,smsfaq.html – Maart 2011

[6] Dreamfabric, http://www.dreamfabric.com/sms/ - Mei 2011

[7] Rashmi Bajaj, Samantha Lalinda, Ranaweera, Dharma P. Agrawal, *GPS: Location-tracking technology.* Web reference: http://cens.ucla.edu/~mhr/cs219/location/agrawal02.pdf - Mei 2011